Seminário

A Assinatura Electrónica
Teoria e Prática

Lisboa, 25 de Outubro de 2002

Organização do Conselho Geral

Nota Prévia : Parte deste documento foi adaptado do manual do Curso online "Advogados Tribunais e E-mail" disponível no Centro de Formação Online do Conselho Distrital de Lisboa
(**http://www.formare.pt/cdl**).
Os conteúdos sobre a utilização prática do Certificado Digital foram disponibilizados pela Multicert.

Índice do Manual

I - Introdução

Introdução

Como todos sabemos e é por todos aceite quase sem reticências, um dos grandes motores de desenvolvimento do presente século será a Internet, bem como todas as potencialidades que lhe são inerentes. Já não é só o computador em si, mas também as formas de comunicação de informação que são possíveis de realizar com ele.

Perante tal cenário, a melhor resposta que se poderia esperar do actual sistema judiciário era a possibilidade de os advogados passarem a poder enviar as suas peças processuais através do e-mail, com todas as vantagens que daí advêm.

Tal medida, que tem como principal objectivo (pensamos nós), uma maior celeridade no processo judicial e no tratamento do mesmo pelos tribunais, tem como base uma das várias alterações ao Código de Processo Civil, mais concretamente a que foi realizada pelo DL 183/200 de 10 de Agosto, entre outras, ao artigo 150.º do código em causa.

No entanto, a aplicabilidade prática da alteração referida só será uma realidade em 1 de Janeiro de 2003, dia a partir do qual o referido diploma entra em vigor.

Contudo, como nos cabe a todos fazer a utilização dessa potencialidade, contribuindo assim para a maior celeridade da justiça, bem como para que não percamos tanto tempo em deslocações na entrega dos nossos trabalhos, é importante que todos estejamos preparados antes dessa data.

O presente manual visa:

1. Proporcionar aos advogados os conhecimentos informáticos que lhes permitam fazer uso da funcionalidade, e como não poderia deixar de ser, estes passarão obviamente pelo uso do e-mail e pela obtenção e utilização de uma assinatura digital.

2. Familiarizar os advogados com as alterações legais realizadas e com o regime jurídico daí decorrente.

Como compreenderão, para que estes objectivos se realizem na sua plenitude é necessário que apreendamos um conjunto de mecanismos que permitam torná-los realidade. Podemos enumerá-los:

- Conhecer e utilizar as potencialidades do e-mail;
- Como obter e aplicar uma assinatura digital;
- Conhecer o regime jurídico de forma a que possamos tomar as decisões correctas mediante as mais diversas situações.

II - O suporte digital (o e-mail)

Objectivos	**Os vários tipos de suporte digital** **Introdução ao E-Mail** **Descrição do funcionamento do Outlook Express** **Inserção de um ficheiro anexo (attach file)**

Os vários tipos de suporte digital

Nos termos da Portaria n.º 1178-E/2000, de 15 de Setembro, que regulamenta aspectos técnicos advenientes das inovações impostas pelo Dec. Lei n.º 183/2000, de 10/08, as peças processuais apresentadas em suporte digital devem sê-lo em disquete, CD-Rom ou correio electrónico.

Permite-nos, pois, a lei que o suporte digital obedeça a uma das três formas:

- Disquete;
- CD-Rom;
- Correio Electrónico.

No presente apenas nos deteremos na análise e conhecimento do correio electrónico, vulgarmente denominado como e-mail.

Introdução ao e-mail

O e-mail (abreviatura de correio electrónico) é a aplicação mais comum utilizada por pessoas, companhias e associações, utilizada em comunicações mediadas por computador. Os sistemas de e-mail permitem enviar e receber mensagens na forma electrónica entre computadores separados por grandes distâncias como as que poderão existir entre um escritório e um tribunal.

Assim sendo, e no sentido de se dar cumprimento ao estabelecido no artigo 150.º/2 do Código de Processo Civil e fazendo uso dessa possibilidade, iremos neste manual transmitir os conhecimentos básicos necessários à utilização do e-mail de forma a que os participantes possam a partir de 1 de Janeiro de 2003 enviar as suas peças processuais por e-mail, através de ficheiros de texto, com todas as vantagens que daí possam resultar.

Existem centenas de programas de software para leitura de correio electrónico, vulgarmente designados por clientes de email. Para os propósitos deste manual iremos abordar o *Microsoft Outlook Express*, que é fornecido com os sistemas operativos Windows da Microsoft. As suas funcionalidades são comuns a muitos outros programas com o mesmo objectivo : ler e escrever mensagens de correio electrónico.

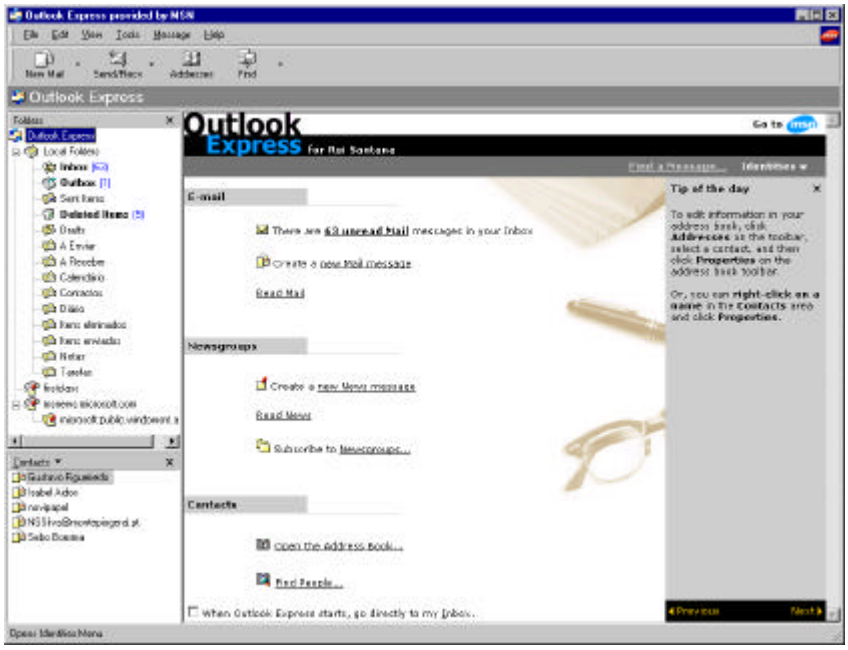
A utilização do Outlook Express

Para se aceder ao Outlook Express, basta clicar duas vezes seguidas na figura que a seguir se apresenta :

E o Outlook Express arrancará automaticamente.

O ambiente do Outlook Express

O Outlook Express apresenta um interface intuitivo com as funcionalidades necessárias ao seu funcionamento presentes no écran inicial que a seguinte imagem representa:

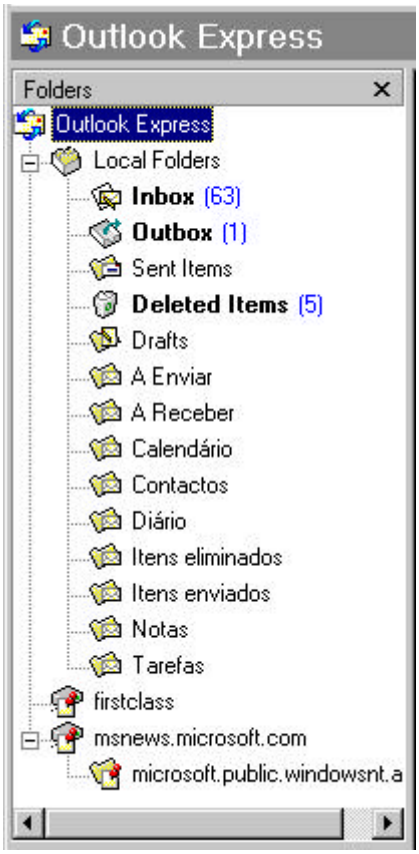


O Outlook Express é composto pelas seguintes funcionalidades:

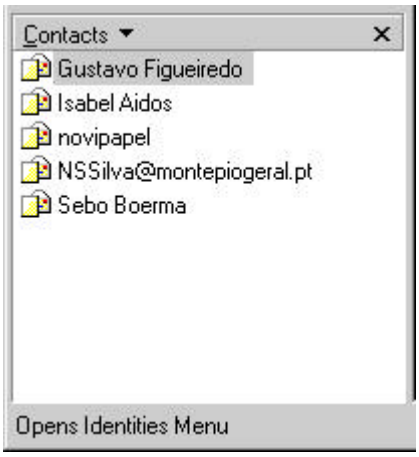
Menu em Texto

Menu Gráfico

Caixa de Directório de pastas



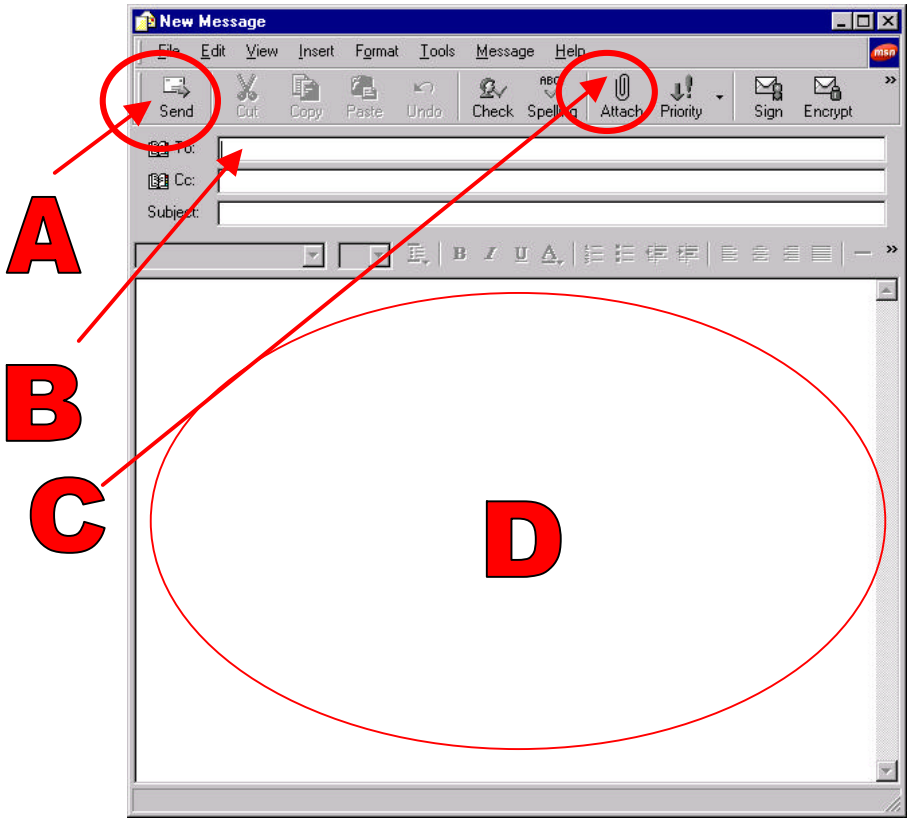
Caixa de Contactos em arquivo



Como enviar e-mail?

Para se enviar e-mail com o Outlook Express, clica-se na opção "New Mail" da barra de opções gráfica (note-se que existe sempre uma opção correspondente no menu de texto)

Automaticamente abre-se a seguinte caixa de envio de mensagens:



Cada área funcional (representada por uma letra) tem a seguinte característica:

A – Envio da mensagem quando se terminar o texto a enviar. Logo que se termina de escrever o texto da mensagem, o endereço do seu destinatário, o assunto e a inserção de eventuais anexos, é nesta opção que se clica, o que activa o mecanismo de colocar a mensagem em lista de envio. Note-se que nesta fase a mensagem não é ainda enviada. Explicaremos mais tarde como se enviam todas as mensagens que estão em lista de envio.

B – Endereço do destinatário. É aqui que se regista o endereço de quem irá receber a mensagem. O formato de um endereço tem sempre a forma XXX@YYY.ZZZ, onde XXX representa o nome da pessoa registada em email, YYY o domínio onde está registada e ZZZ pode ser um país, ou outras terminações genéricas (por exemplo .com , .net, .edu, etc...). No caso de uma conta disponibilizada pela OA com a forma :

o-seu-endereco-99999H@adv.oa.pt, temos que :

o-seu-endereco-9999H é um utilizador registado e reconhecido num determinado servidor de correio. O símbolo "@" que originalmente era referido em inglês "at" e foi assimilado com a designação "arroba" separa o utilizador do servidor, isto é, xxxx@oninet.pt é, em termos de endereço electrónico completamente diferente de xxx@netcabo.pt. Voltando às contas disponibilizadas pela OA temos que o utilizador está registado num servidor que é reconhecido na Internet por adv.oa.pt .

Quando uma mensagem é enviada, os equipamentos que asseguram o transporte e entrega das mensagens na Internet lêem o endereço de destino da direita para a esquerda fazendo validações de nomes tentando encontrar o servidor que guarda as mensagens do destinatário. Com as contas da OA :

o-seu-endereco-99999H@adv.oa.pt

pt é válido ? Sim pt é a terminação de Portugal na Internet.

oa.pt é válido ? Sim e aqui já é a entidade que gere os domínios em pt (a Fundação para a Computação Científica Nacional – FCCN) que responde pela validade.

adv.oa.pt é válido ? Sim e essa validade já tem que ser demonstrada pelo servidor oa.pt .

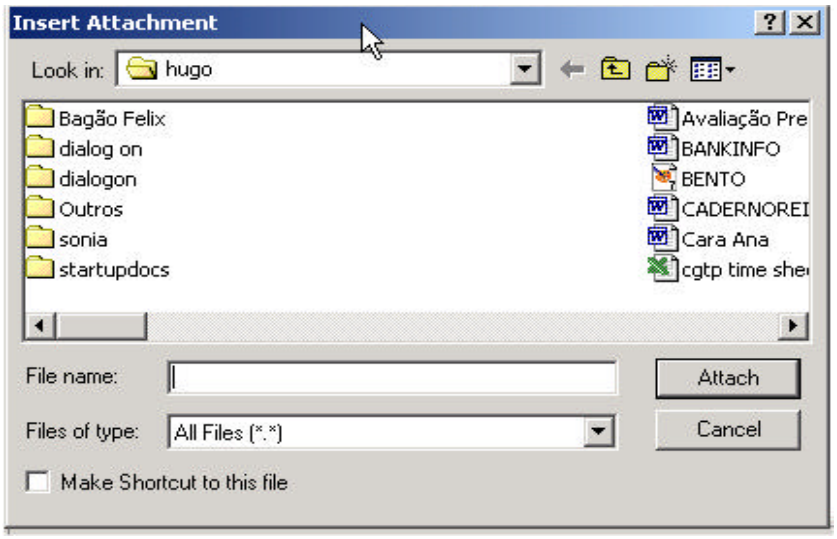
o-seu-endereco-99999H é um utilizador do servidor adv.oa.pt ? Sim e a mensagem é entregue ao servidor ficando a aguardar que o dito utilizador a leia e transfira para o seu PC.

C – Anexos. Sempre que se pretender enviar ficheiros anexos à mensagem, clica-se neste botão que chamará uma caixa onde poderemos escolher o ficheiro que pretendemos anexar.

D – Zona de escrita da mensagem. É aqui que escrevemos o texto da mensagem que pretendemos enviar.

Voltando ao ponto C e aos ficheiros anexos, relembramos que cada vez que se pretender enviar uma peça processual para um tribunal, em formato de texto (é obrigatório utilizar o formato RTF. Pode gravar um documento do word neste formato), terá que se utilizar a funcionalidade acima referida.

Clicando no botão acima indicado, aparecerá uma caixa como a que se segue:



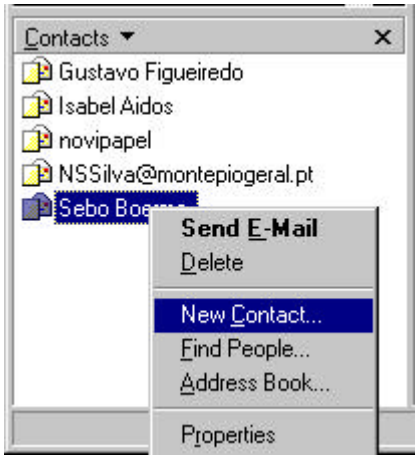
Em seguida deverá seleccionar o ficheiro que pretende enviar anexo à mensagem, procurando-o na directoria respectiva.

Depois clicará no botão “abrir” e o ficheiro seleccionado seguirá como anexo à sua mensagem.

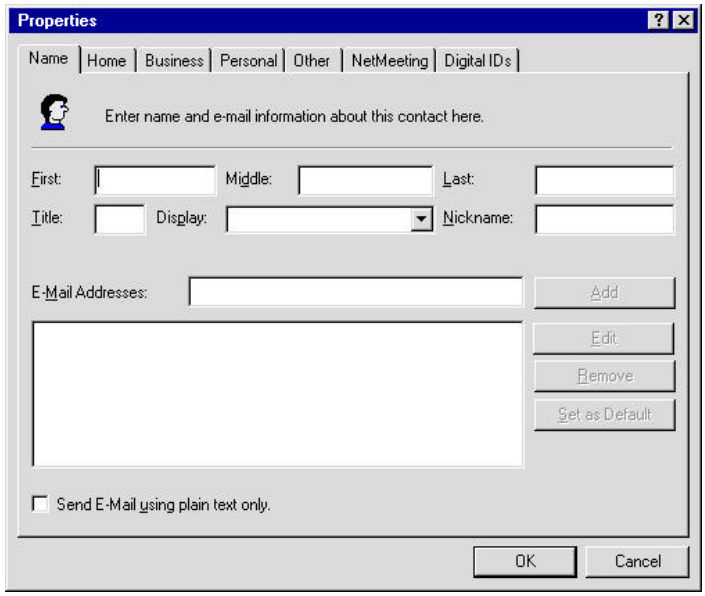
Por fim envia a mensagem e com ela segue o ficheiro anexado.

Particularidades da caixa de contactos

Muitas vezes não nos lembramos do endereço de email de uma pessoa. Para isso o Outlook Express possui um sistema que arquiva contactos para posterior utilização. O envio de mensagens fica desta forma simplificado pois basta clicar duplamente no nome do destinatário que aparecerá uma caixa idêntica à do envio de uma nova mensagem, mas já com o endereço do destinatário escolhido. O resto do processo desenrola-se como se fosse uma mensagem nova.



Neste sistema, se clicar com o botão do lado direito do obtém-se um menu de opções que permite gerir a lista de contactos.
Para adicionar um contacto novo, basta escolher a opção “New Contact” e aparecerá a seguinte ficha de registo

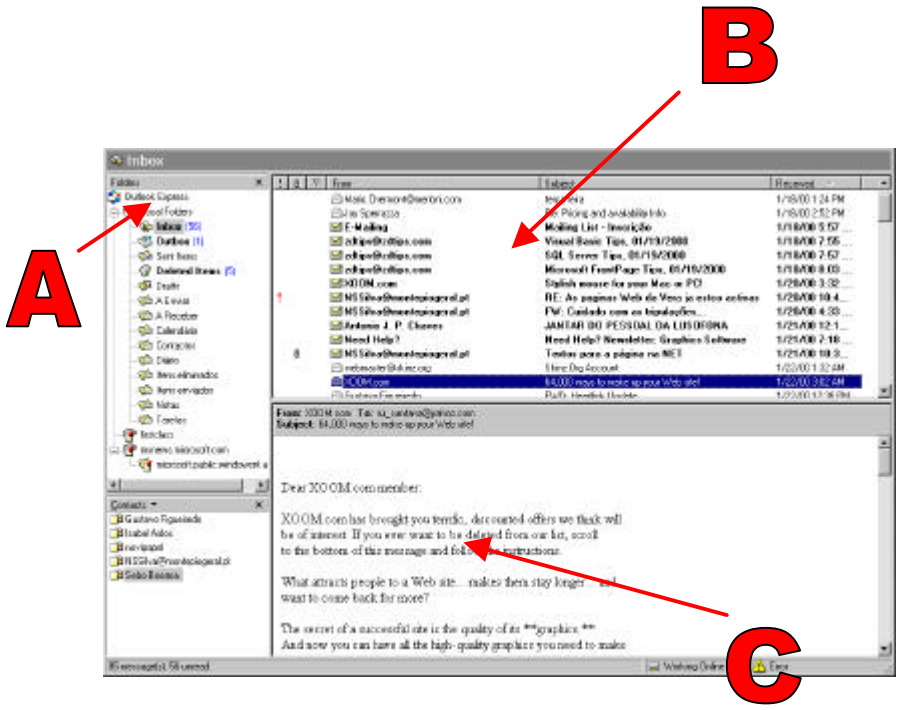


Podem ser registadas várias informações que servirão de registo a posteriores contactos e funciona como uma agenda de contactos.

Leitura de mensagens recebidas

A leitura de mensagens é feita de uma forma muito simples.

A caixa de árvore de directórios mostra uma pasta com o nome “Inbox” (A), a qual representa a caixa de correio recebido.



Se escolhermos esta pasta a janela lateral apresentará uma lista de mensagens em arquivo (B).

A visualização das mensagens efectua-se clicando na mensagem que se pretende ver, o que automaticamente apresentará o seu conteúdo na janela inferior (C).

III - Assinatura Digital e a sua Certificacão

Objectivos	**Assinatura digital** **Certificado digital** **Processo de certificação** **Obtenção de email e Certificado Digital**

1. Introdução

De acordo com o disposto no artigo 150.º/2 c) do Código de Processo Civil, para que a peça processual enviada por correio electrónico (E-mail) seja válida, será necessária a aposição de assinatura digital do signatário da mensagem.

Portanto, após estudarmos, no capítulo anterior os procedimentos informáticos que nos permitem enviar a mensagem contendo a peça processual, cabe agora no presente capítulo estudarmos os procedimentos necessários à obtenção de uma assinatura digital, bem como a sua aposição numa determinada mensagem.

Antes de mais, lembramos que o diploma legal aplicável a esta matéria é o Decreto-Lei n.º 290-D/99 de 2 de Agosto, que regulamenta a validade, eficácia e valor probatório dos documentos electrónicos e assinatura digital.

2. A assinatura digital

De acordo com o diploma supra referido, assinatura digital é:

"processo de assinatura electrónica baseado em sistema criptográfico assimétrico composto de um algoritmo ou série de algoritmos, mediante o qual é gerado um par de chaves assimétricas exclusivas e interdependentes, uma privada e outra pública, e que permite ao titular usar a chave privada para declarar a autoria do documento electrónico ao qual a assinatura é aposta e concordância com o seu conteúdo, e ao declaratário usar a chave pública para verificar se a assinatura foi criada mediante o uso da correspondente chave privada e se o documento electrónico foi alterado depois de aposta a assinatura" (Cfr art 2.º do Decreto-Lei n.º 290-D/99 de 2 de Agosto).

Tal como a assinatura tradicional é utilizada em documentos em papel, as assinaturas digitais começam a ser utilizadas para identificação de autoria de documentos electrónicos, com o mesmo significado e o mesmo grau de importância.

Contudo as assinatura electrónicas que servem de base às digitais, devem de acordo com a lei:

- Identificar de forma unívoca o autor do documento;
- Mostrar que a sua aposição ao documento resultou da vontade do autor;
- Detectar através da sua conexão com o documento se existe qualquer alteração superveniente ao envio do mesmo.

As assinaturas digitais são criadas utilizando a chave privada do titular. Posteriormente são verificadas pelo receptor utilizando a chave pública do titular da assinatura, a qual se encontra no Certificado Digital emitido em seu nome.

Para assinar digitalmente qualquer tipo de documento electrónico a fim de comprovar inequivocamente a autoria do mesmo, o utilizador deverá possuir um Certificado Digital, único e pessoal, que comprove indubitavelmente a sua identidade no mundo electrónico e que tenha sido emitido por uma entidade certificadora de confiança, devidamente fiscalizada e credenciada nos termos do Decreto-Lei n.º 290-D/99 de 2 de Agosto.

Podemos deter como definição de **assinatura**, numa acepção ampla, qualquer sinal ou acto pelo qual o autor de um documento se identifica e manifesta a sua concordância com o conteúdo declarativo dele constante, isto é, o meio de autenticação pelo próprio autor do documento por ele gerado.

Assinatura Digital é, pois, uma modalidade de assinatura electrónica que consiste num «selo electrónico» que é acrescentado a um documento e que é criado através de um sistema criptográfico assimétrico, que gera e atribui ao respectivo titular uma chave privada e uma chave pública.

São elementos constitutivos do regime da assinatura digital:

- A existência de um par de chaves criptográficas, pública e privada;
- A utilização da chave privada para geração da assimetria digital;
- A correspondência necessária da chave privada à chave pública;
- A emissão de um Certificado que contenha a chave pública;
- A emissão de um Certificado que contenha a chave pública, por uma entidade certificadora credenciada nos termos do diploma;
- A validade do Certificado, quer quanto à sua emissão, quer por não estar suspenso, nem revogado, nem caduco por ultrapassagem do seu prazo de validade.

Atendendo ao regime legal aplicável, o **valor jurídico da assinatura digital** é, nos termos do artigo 7º do Decreto-Lei n.º 290-D/99, equiparado à assinatura autógrafa tradicional, consagrando a presunção legal, ilidível por prova em contrário, de que o documento electrónico ao qual foi aposta uma assinatura

digital se verificam as três funções destas e os correspondentes efeitos práticos e jurídicos, nomeadamente:

- Função identificadora: a assinatura identifica inequivocamente a autoria do documento;
- Função finalizadora: comprova o assentimento do signatário às declarações de vontade constantes do documento;
- Função de inalterabilidade: comprova que o documento não foi alterado após a aposição da assinatura até à sua recepção pelo destinatário.

3. O Certificado Digital

De acordo com a lei, o Certificado Digital é um documento electrónico autenticado com assinatura digital que certifica a titularidade de uma chave pública e a sua validade.

Esse documento é emitido por uma entidade certificadora que cria e assina um Certificado Digital, um documento electrónico que associa inequivocamente a identidade de um indivíduo ou organização a uma chave pública assegurando a sua legalidade e fiabilidade.

Cada utilizador de um Certificado possui um par de chaves, e através da utilização de uma ou de outra, conseguem-se garantir valores nas mensagens tão importantes como a autenticidade, integridade, aceitação e confidencialidade.

Este par de chaves (chave pública/chave privada) em princípio não tem qualquer associação directa a uma identidade pessoal. É simplesmente um conjunto de números.

Para que a criptografia de chaves públicas seja um sucesso, é necessária uma terceira entidade de confiança que relacione inequivocamente uma identidade

com o par de chaves. Esta entidade é denominada por Entidade Certificadora devidamente fiscalizada e tutelada por uma Autoridade Credenciadora.

Assim, um Certificado Digital pode ser utilizado como forma de identificação digital, como um BI por exemplo, podendo ser utilizado para efectuar transacções electrónicas em redes abertas com segurança e privacidade, assinar digitalmente documentos e disponibilizar outros mecanismos para fins de confidencialidade, como é o caso do envio de uma peça processual para um tribunal.

4. Processo de certificação

Foi graças à criptografia que se resolveram os problemas de segurança associados às transacções electrónicas no mundo digital.

A criptografia assegura a protecção da informação usando uma função matemática ou algoritmo para encriptar e desencriptar mensagens.

Um algoritmo simples consegue esconder cada caracter de um texto, trocando duas letras. Por exemplo, um A passa a C, um B passa a D, um S passa a A, etc.

Na generalidade existem dois tipos de algoritmos criptográficos:

- os simétricos, ou convencionais, em que só existe uma chave para encriptar e desencriptar;
- os assimétricos, ou de chave pública, em que existem duas chaves diferentes, matematicamente relacionadas (Pública e Privada).

O princípio base a ter em conta relativamente às relações existentes entre as duas chaves é a seguinte:

O que uma encripta só a outra desencripta.

Ou seja :

- Qualquer informação encriptada pela chave privada só é desencriptada pela *chave pública* correspondente (do par);

- Qualquer informação encriptada pela chave pública só é desencriptada pela chave privada correspondente (do par).

Confidencialidade

Num sistema de **encriptação por chave pública**, a informação é encriptada com a chave pública da pessoa a quem é dirigida a mensagem e só a pessoa que tem a chave privada correspondente (o destinatário correcto) é que consegue desencriptar a mensagem. Este é o caso de um advogado que pretende enviar uma peça processual para um tribunal garantindo a sua total confidencialidade. Para isso terá que encriptar a mensagem com a chave pública desse tribunal.

É importante esclarecer que a encriptação de mensagens não é obrigatória. A simples aposição de uma assinatura digital garante ao destinatário que a mensagem não foi alterada desde o seu envio. Não garante, no entanto, que a mesma não foi visualizada desde o envio à recepção. Somente nos casos em que o conteúdo da mensagem a enviar é de tal forma confidencial que a visualização por terceiros pode acarretar prejuízos graves, é que se deve utilizar a funcionalidade de encriptação. Além de assinada a mensagem será encriptada, garantindo a impossibilidade da sua leitura por qualquer outra entidade que não o seu destinatário. Recorde que para poder enviar uma mensagem encriptada terá que possuir a chave pública do destinatário. O acesso a essa chave pública é normalmente garantido pelas entidades emissoras dos Certificados Digitais que são obrigadas a manter acessível um repositório de chaves públicas.

Com o sistema de chave pública, tanto o remetente como o destinatário podem, de uma forma segura, trocar informação privada numa transacção electrónica.

Integridade e Assinatura digital

Uma assinatura digital é um "selo electrónico" que pode ser enviado durante qualquer transacção electrónica. Semelhante a um selo de um pacote de encomenda, a assinatura digital previne contra alguém que deseje alterar quer o conteúdo da informação, quer os dados do verdadeiro emissor e autor do documento.

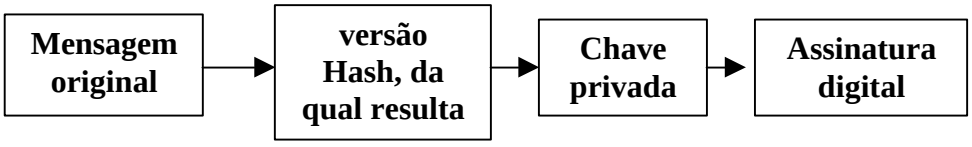
Qualquer mudança na informação, nem que seja uma vírgula, será detectada quando essa assinatura digital for verificada.

Para criar uma assinatura digital é necessário primeiro que o emissor da mensagem gere uma versão da mensagem conhecida por código Hash ou código da mensagem.

Este código, gerado por algoritmos públicos, é único para o texto original. Qualquer alteração no texto original é suficiente para que o código gerado seja completamente diferente.

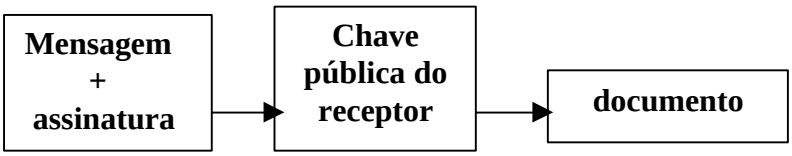
O emissor cria a assinatura digital ao assinar (encriptar), posteriormente, o código *Hash* da mensagem com a sua chave privada.

O esquema seguinte mostra-nos como se apõe uma assinatura digital numa mensagem.



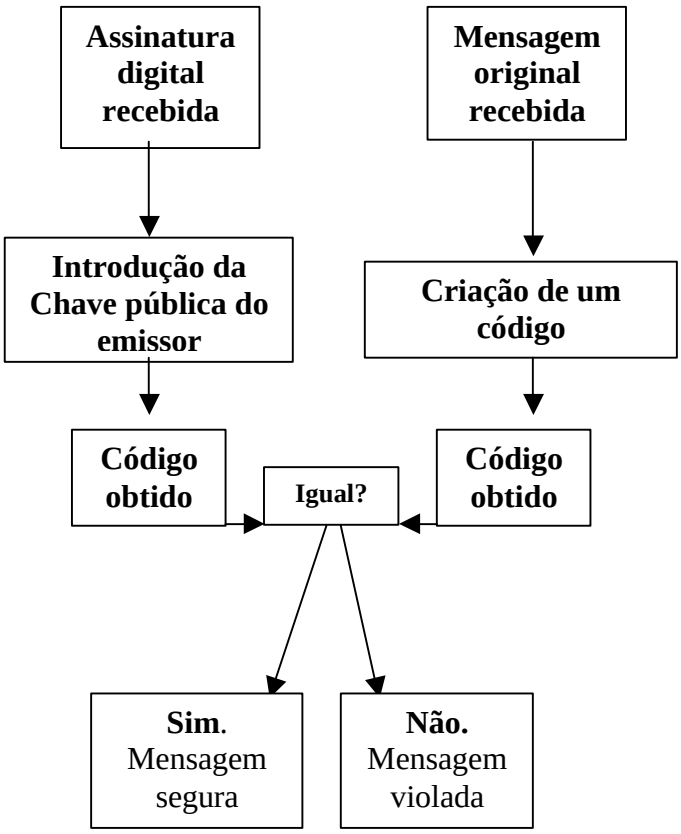
Com o objectivo de mais ninguém ter acesso ao conteúdo da mensagem, a não ser o correcto receptor, isto é, para garantir a confidencialidade na transmissão da informação contida no documento, o emissor da mensagem adiciona a assinatura digital criada à mensagem original, que encripta, por sua vez, com a chave pública do receptor. É criada, assim, uma mensagem electrónica confidencial e assinada digitalmente.

O esquema seguinte mostra-nos como funciona o processo de encriptação de uma mensagem pelo seu emissor:



Após a recepção da mensagem, o receptor acede ao texto utilizando a sua chave pública. A fim de obter a assinatura digital original em formato legível, o receptor desencripta o código Hash recebido com a chave pública do emissor. Para verificar a exactidão da assinatura digital e a integridade da informação, o receptor gera um código Hash com a mensagem original que recebeu, e compara este código com o que obteve da desencriptação da assinatura digital recebida. Se o receptor validar positivamente a assinatura digital com a chave pública do emissor, temos um forte indicador de que a mensagem foi enviada pelo dono da chave privada e que, simultaneamente, não foi alterada no seu trajecto.

O esquema seguinte mostra-nos o processo de validação de uma mensagem assinada digitalmente:



Isto implica então o seguinte: que o emissor possua a chave pública do receptor e vice-versa.

Certificado Digital

Como podemos ter a certeza de que o par de chaves (pública e privada) pertence realmente a um determinado emissor?

A reposta é simples: através da utilização de Certificados Digitais, emitidos por uma terceira parte legalmente credenciada.

Antes de duas partes trocarem informação usando encriptação de chaves públicas, cada uma delas, deseja autenticar a identidade da outra parte. Por

exemplo os remetentes querem saber se estão a lidar realmente com o destinatário eleito. Obviamente que os destinatários também querem ter a certeza da identidade dos seus remetentes e da exactidão das informações trocadas.
Uma forma de assegurar a autenticação de cada uma das partes pode ser alcançada através dos serviços de uma terceira parte (a entidade certificadora) que emite e regula os serviços de gestão e emissão de *certificados digitais*.

Para criar um Certificado Digital, a Entidade Certificadora cria um código Hash com, entre outros dados, a informação da identidade do utilizador e a sua chave pública. A Entidade Certificadora «assina» esta informação ao utilizar a sua chave privada (da Entidade Certificadora), criando um código Hash encriptado. Esta informação é, desta forma, incluída no Certificado a emitir.

Se a informação da identidade do utilizador, ou a chave pública contida no *Certificado Digital*, for alterada de qualquer forma, o Certificado é detectado como inválido.

Para confirmar a integridade de um Certificado Digital, o receptor:

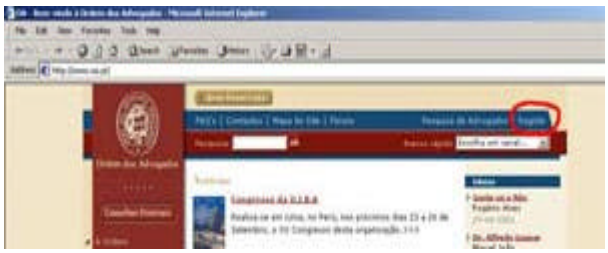
- Recria o código Hash usando o mesmo algoritmo e informação que a Entidade Certificadora utilizou na criação do Hash original para o Certificado em questão;
- Desencripta o Hash existente no Certificado Digital com a Chave Pública da Entidade Certificadora;
- Compara os dois valores obtidos (códigos Hash), e se estes forem iguais o Certificado Digital presume-se íntegro. Caso contrário, o Certificado Digital sofreu alterações e é inválido.

Observação: Utilizando, o MS Outlook esta acção é processada automaticamente e de forma transparente para o utilizador.

5. Onde e como posso obter um Certificado Digital?

Procedimentos a executar:

1º No Portal da Ordem dos Advogados, deverá proceder ao seu registo (www.oa.pt).



Clicando em "Registo" na página inicial, preenchendo de seguida o formulário.

Serão aceites registos de Advogados e Advogados Estagiários na 2ª Fase do Estágio. As Sociedades de Advogados deverão fazer o pedido através do endereço de correio electrónico para mail.soc@cg.oa.pt. Receberá uma mensagem a agradecer a sua participação. **O processo de registo está completo.**

2º Receberá uma carta registada com aviso de recepção (no seu domicílio profissional) que contém :

A) Dados necessários para a configuração de uma conta de correio electrónico (exemplo de carta tipo) :

«Ex.mo(a). Sr(a). Dr(a).
Francisco Pedro Matias
Lg S. Domingos 14-1º
1069-060Lisboa

Exmo(a). Sr(a). Dr(a).

Junto enviamos os dados necessários para configurar a conta de correio electrónico no sub-domínio adv.oa.pt
A conta já está activa e pode começar a ser utilizada assim que efectue as configurações necessárias.

Nome de Utilizador : x00000
Palavra Passe : 3Lk7tyg

Cédula: 99999h
Endereço de correio electrónico pré-configurado: x00000-99999h@adv.oa.pt

Nome de Utilizador : x00000
Palavra Passe : 3Lk7tyg

Configurações técnicas:
Servidor de Correio a Receber (POP3) : adv.oa.pt
Servidor de Correio a Enviar (SMTP) : o do ISP que utiliza na sua ligação à Internet.»

B) Carta de PIN com a informação para obter o Certificado Digital (idêntica às cartas que recebe com o PIN de um cartão Multibanco).

3º Utilizando a informação recebida, deverá aceder à Área Reservada do Portal da Ordem dos Advogados.

O acesso faz-se utilizando o "Nome de utilizador" e a "Palavra passe" quando clicar no Portal em "Área Reservada".

Na Área Reservada escolhendo "Serviços on-line" poderá :

a) Personalizar o seu endereço de correio electrónico :
O endereço de correio electrónico terá a forma xxxxx-99999h@adv.oa.pt para Advogados ou xxxxx-99999h@adv-est.oa.pt para Advogados Estagiários onde xxxxx é completamente personalizável e 99999h é o nº de cédula e respectivo Conselho Distrital.

NOTA MUITO IMPORTANTE

Um Certificado Digital é emitido para um endereço de correio electrónico. A alteração de endereço invalida o Certificado Digital. Quando efectuar a personalização do seu endereço de correio electrónico está a escolher o endereço para o qual será emitido o Certificado.
Tenha isso em consideração uma vez que após gerar o Certificado para o endereço de correio electrónico que personalizou não poderá alterar o seu endereço sob pena de o Certificado emitido ser revogado tendo que proceder ao pedido de emissão de um novo Certificado, o qual já não beneficiará das condições especiais acordadas entre a Ordem e a Multicert (gratuitidade durante o primeiro ano).

b) Alterar a palavra passe associada ao nome de utilizador.

No caso de já lhe ter sido atribuído um endereço de correio electrónico no sub-domínio “advogados.oa.pt” e o quiser manter na página de personalização de endereço de correio electrónico dará essa indicação.

Como obter um Certificado Digital

1º- Após terminar a personalização do endereço de correio electrónico na Área Reservada (tal como está explicado) será reencaminhado para uma página onde após tomar conhecimento das Condições Gerais do Contrato de Emissão de Certificado Digital Individual formaliza o pedido de emissão do seu Certificado Digital. Após algumas horas receberá uma mensagem, via email, com o endereço de uma página Web onde se identifica utilizando os dados constantes da carta de PIN e o seu endereço de correio electrónico (que já deverá ter personalizado).

2º- Receberá depois no seu endereço de correio electrónico as instruções que lhe permitem fazer a recolha do Certificado Digital para o seu computador.

IV – Configuração das contas de correio electrónico

Após concluída a personalização terá que configurar o seu programa de correio electrónico para que possa utilizar a conta que acabou de personalizar.

Como exemplo, ficam os passos necessários para configurar o Microsoft Outlook Express.

Ao abrir o "Outlook Express" pela 1ª vez irá surgir automaticamente o Assistente de Ligação. Ser-lhe-á pedida a informação necessária à configuração da sua caixa de correio.

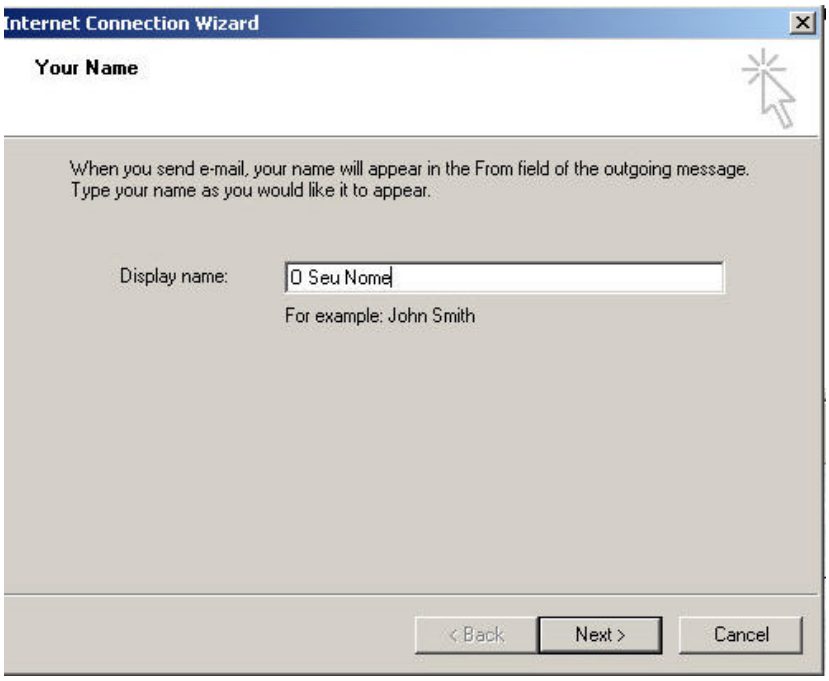
Caso não surja este assistente e/ou pretenda adicionar um novo serviço de correio ao "Outlook Express", clique no menu "Ferramentas", escolha "Contas...", clique em "Adicionar" e seleccione "Correio...".

Preencha os campos que lhe vão sendo apresentados de acordo com as instruções abaixo indicadas

Em caso de dúvidas/problemas de configuração tem à sua disposição os contactos do Suporte Técnico :

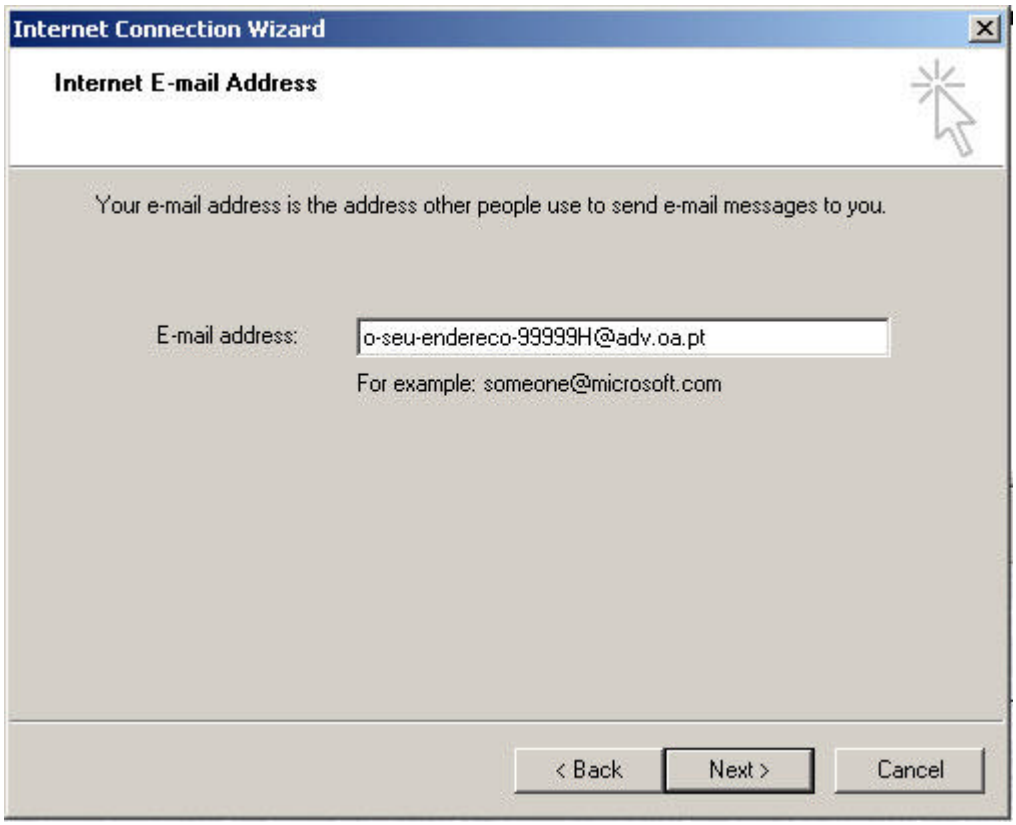
Correio electrónico: suporte@cg.oa.pt (preferencial)

Telf: 218 823 550 (das 10h às 18h, de segunda a sexta)

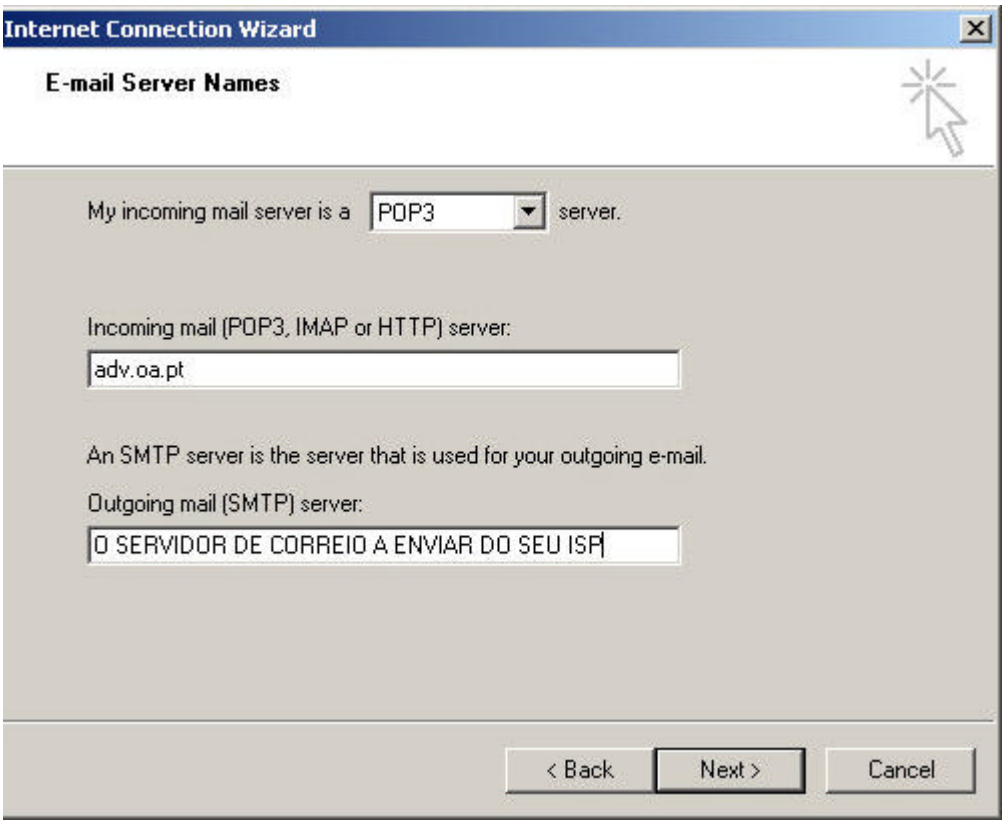


Introduza o nome que quer que conste como o de remetente das suas mensagens.
Clique em "Seguinte".

Escreva o seu endereço de correio electrónico da Ordem dos Advogados (ex: o-seu-endereco-99999H@adv.oa.pt).



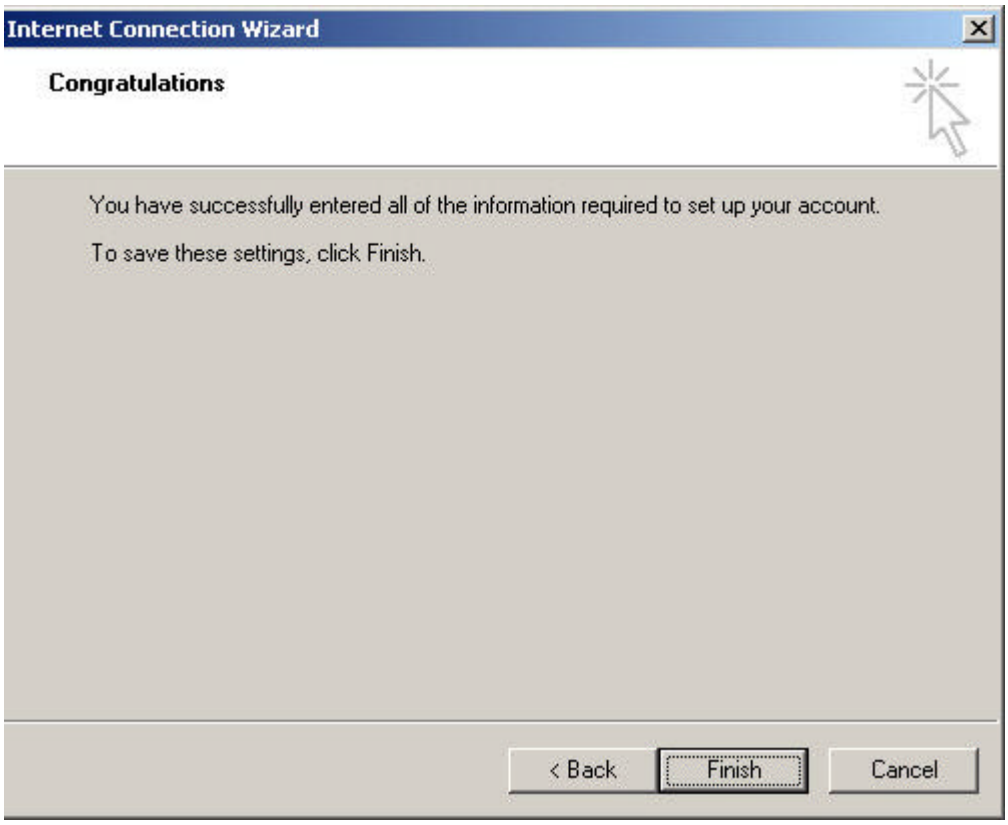
Preencha os campos da imagem que se segue como está no exemplo.



Servidor de correio a receber (POP3)": adv.oa.pt

"Servidor de correio a enviar (SMTP) do seu ISP": mail.telepac.pt, mail2.ip.pt; smtp.oninet.pt; etc...

Introduza o seu Nome de Utilizador e a respectiva Palavra Passe que recebeu na carta enviada pela OA.



Clique em "Terminar".

Parabéns acabou de configurar a sua conta de correio electrónico!

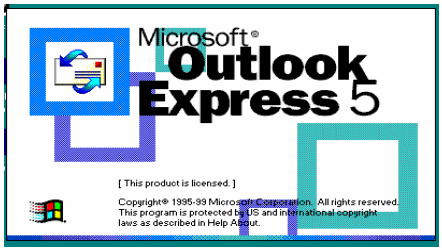
Agora já pode começar a receber e enviar correio electrónico com a conta disponibilizada pela Ordem dos Advogados.

V- Utilização do Certificado Digital

Assinatura Digital de mensagem de Correio Electrónico

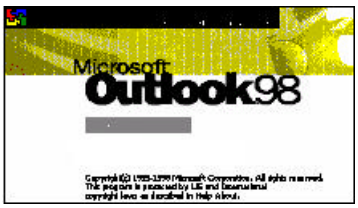
I – Configuração do Cliente de mail
(para a utilização de Certificados)

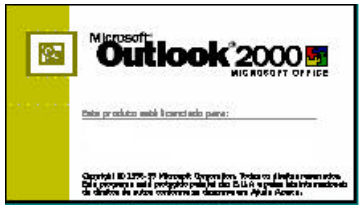
Se o seu programa de e-mail é o **Microsoft Outlook Express 5 e 6**…



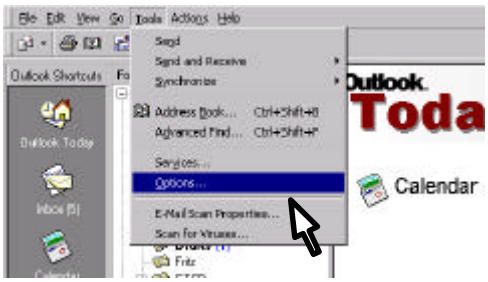
…passe para o capítulo **II – Envio de mensagem assinada**. O Outlook Express, uma vez importados os certificados, não requer qualquer configuração.

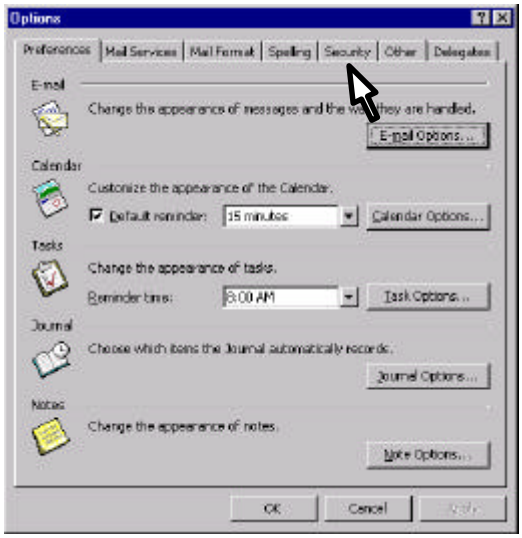
Se o seu programa de e-mail é o **Microsoft Outlook 98** ou o **Microsoft Outlook 2000**…





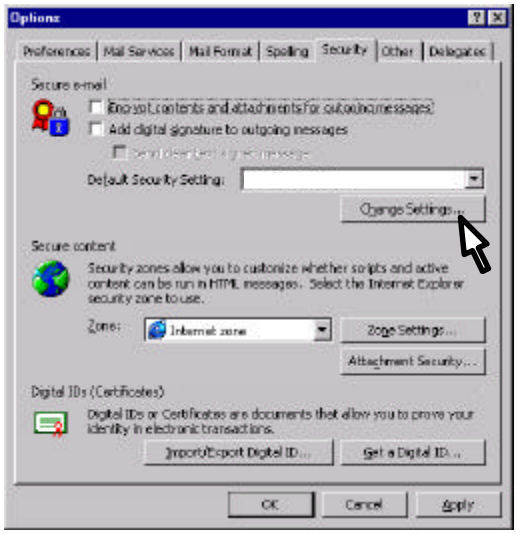
Clique em *Tools (Ferramentas) -> Options (Opções)*



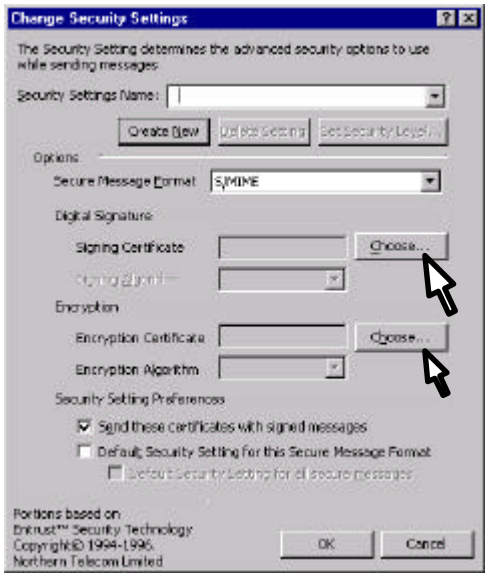


Abra a pasta *Security (Segurança)*

Clique em *Change Settings (Configurar correio electrónico).*
Se pretender que todas as suas mensagens de mail sejam assinadas automaticamente, pode escolher a opção *Add digital signature to outgoing message (Adicionar a assinatura digital às mensagens a enviar).* No caso de escolher esta opção já não necessita de seguir as instruções seguintes, sobre o *Envio de mensagem assinada*.

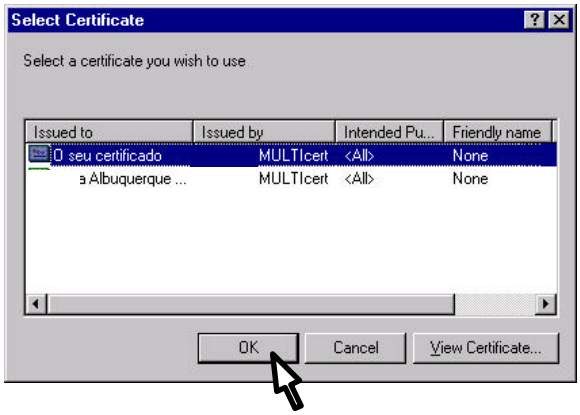


Se escolher a opção *Encrypt contentes and attachments for outgoing messages* (*Codificar conteúdo e anexos de mensagens a enviar*), tenha em atenção que para codificar a mensagem é necessário ter o Certificado da pessoa para quem quer enviar a mensagem encriptada.



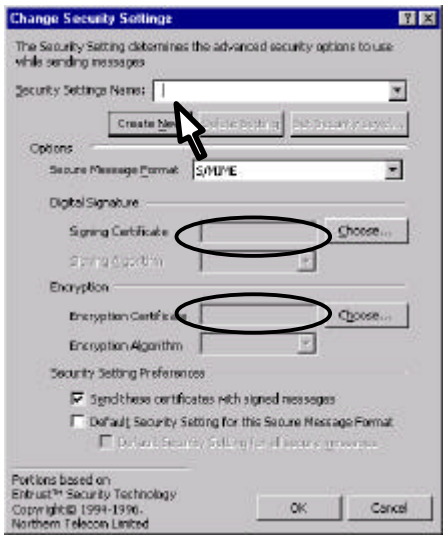
1. Quando clicar no primeiro *Choose (Escolher)* visualizará a janela para escolher o seu Certificado.

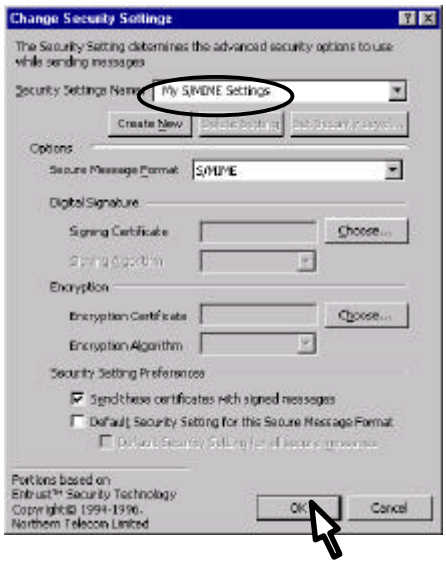
2. Clique no segundo *Choose (Escolher)*. A janela de escolha do Certificado aparece novamente.



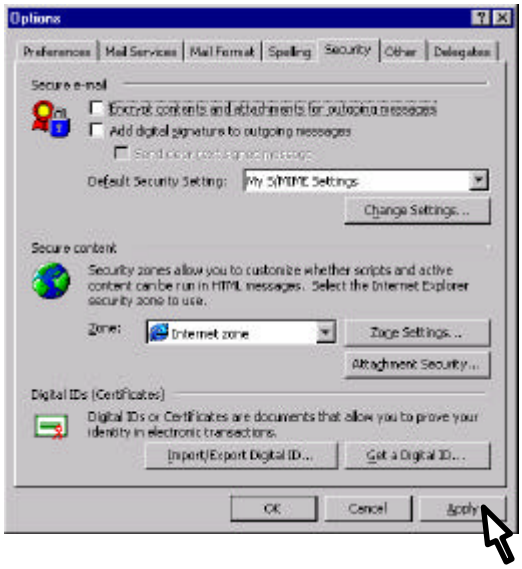
1.a) Seleccione o seu Certificado e clique *OK.*

2.a) Seleccione de novo o seu Certificado e faça *OK.*
Confirme o seu nome nos certificados.
Identifique as definições de segurança *(Security Settings Name / Nome das definições de segurança)* designando-as por exemplo, como "My S/MIME Settings". Clique *OK*…





… e na janela das *Options (Opções)* clique *Apply (Aplicar)* e depois *OK*.

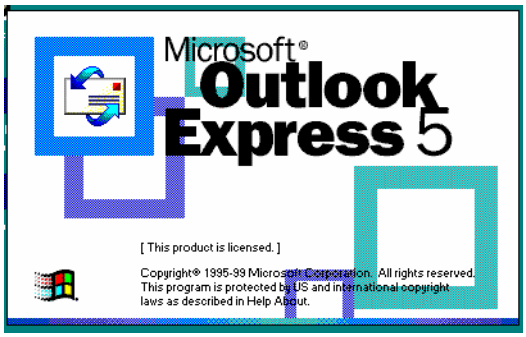


A partir de agora o seu cliente mail está configurado para enviar mensagens assinadas.

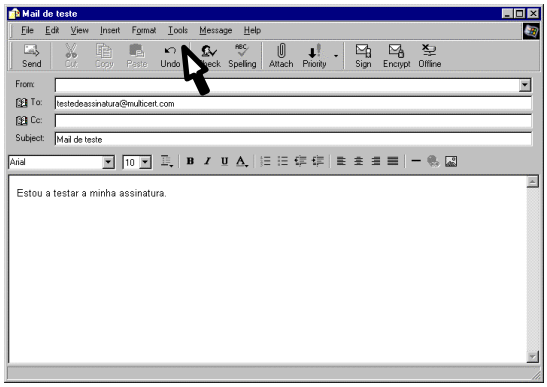
Experimente enviar o seu primeiro mail assinado.
Veja de seguida como pode fazê-lo.

II – Envio de mensagem Assinada

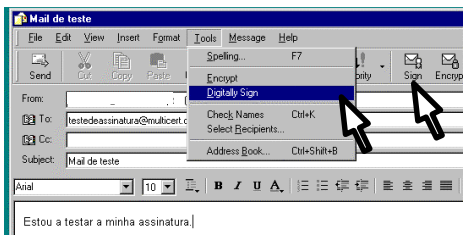
1. Se o seu programa de e-mail é o **Microsoft Outlook Express 5 ou posterior**

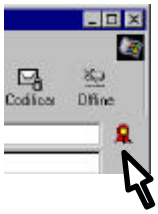


…crie uma nova mensagem.



Clique *Tools (Ferramentas) -> Digital Sign (Assinar Digitalmente)*.
Pode também simplesmente carregar no ícon de *Sign (Assinar)* e a sua mensagem é automaticamente assinada.





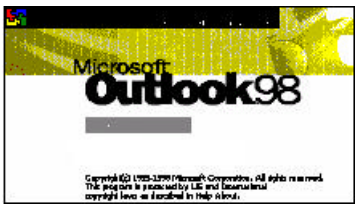
A verificação de que a mensagem está assinada pode fazer-se ao lado dos endereços dos destinatários, quando aparece o ícon respectivo.

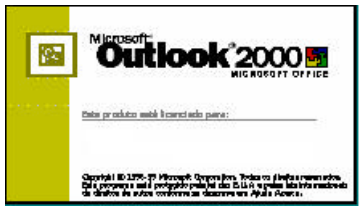
Experimente enviar o seu primeiro mail assinado!

Note que um mail assinado só pode ser lido num programa de mail que esteja preparado para o efeito. O **Outlook97** não está preparado para funcionar com certificados digitais.

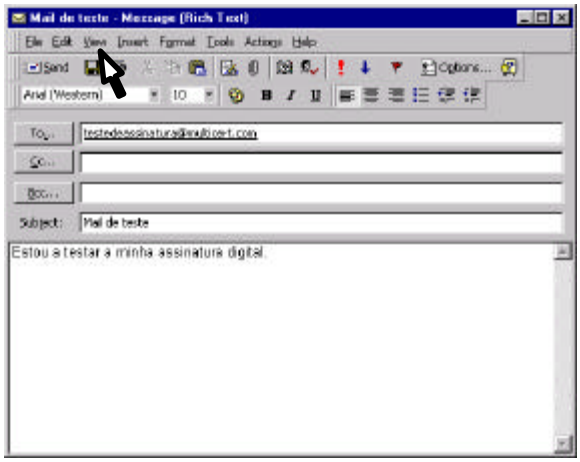
Para actualizar a versão do Outlook que está a utilizar pode gratuitamente aceder à funcionalidade de actualização de produtos do Windows, escolhendo no Internet Explorer a opção “Ferramentas e depois Actualização do Windows”. As actualizações disponíveis para todos os seus programas ser-lhe-ão mostradas e poderá decidir quais é que quer instalar.

2. Se o seu programa de mail é o **Microsoft Outlook 98**, **Microsoft Outlook 2000 ou Microsoft Outlook 2002**…

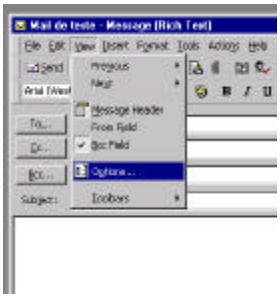




…crie uma nova mensagem.

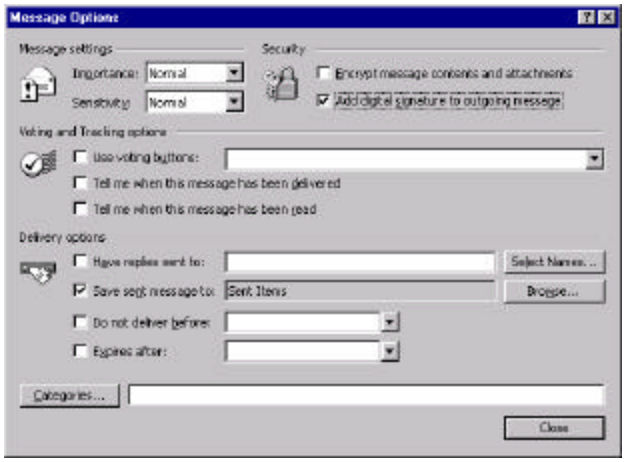


Clique *View (Ver) -> Options (Opções)*



Na janela das opções da mensagem marque (√) a opção *Add digital signature to outgoing message (Adicionar assinatura digital à mensagem a enviar)*.

Se escolher a opção *Encrypt contentes and attachments for outgoing messages* (*Codificar conteúdo e anexos de mensagens a enviar*), tenha em atenção que para codificar a mensagem é necessário ter o Certificado da pessoa para quem se quer enviar.



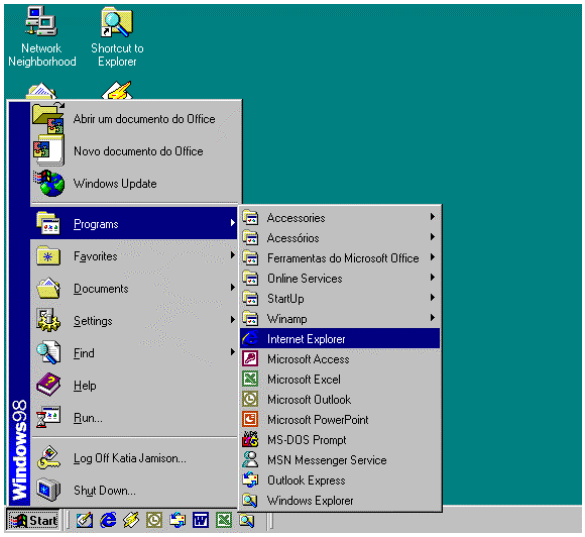
Faça *Close (Fechar)* e envie a sua mensagem normalmente.

Experimente enviar o seu primeiro mail assinado!

Note que um mail assinado só pode ser lido num programa de mail que esteja preparado para o efeito. O Outlook97 não está preparado para funcionar com certificados digitais.

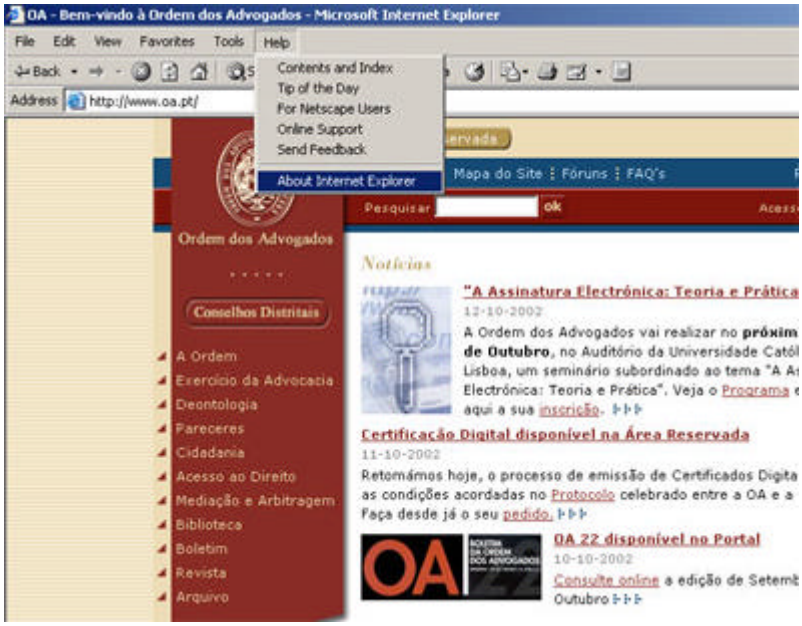
Anexo I – Exportação e Importação de Certificado Digital

I.1 - Abra o seu Browser Internet Explorer, fazendo:



ou fazendo duplo clique em:

I.2 - Uma vez aberto, confirme qual é a versão que tem instalada...



...Se a versão é a **IE5 ou superior** , então siga as instruções, se possuir uma versão anterior deverá proceder à sua actualização tal com foi explicado no capítulo anterior.

Anexo IA – Exportação dos Certificados

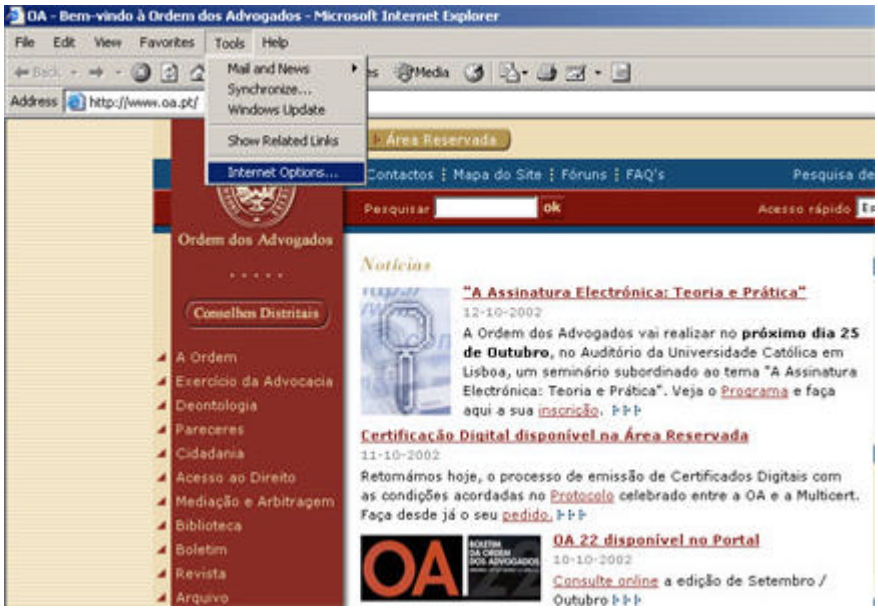
Um Certificado Digital só pode ser gerado uma vez. Qualquer procedimento que inutilize o Certificado Digital (reinstalação do sistema operativo, remoção inadvertida do Certificado Digital, etc..) obriga à emissão de um novo Certificado. É por isso muito importante que exporte o seu Certificado Digital para um suporte externo ao computador onde foi originalmente gerado.

Consegue com este procedimento garantir a integridade do seu Certificado em caso da sua inutilização e ainda a sua instalação em mais do que um computador. A exportação será completada com uma explicação dos procedimentos de importação. Verificará que é um processo simples.

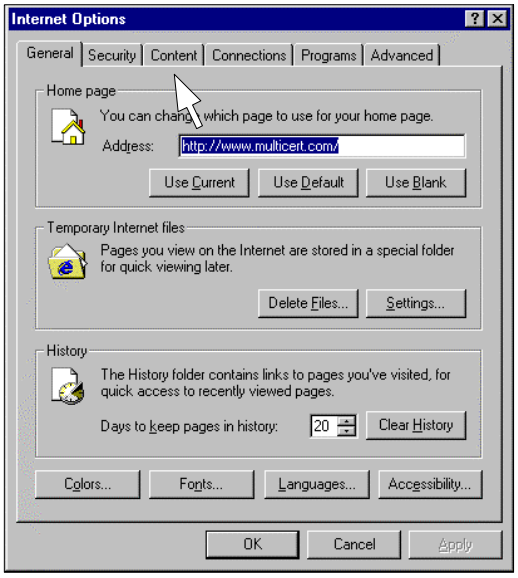
É ainda importante referir que um Certificado Digital pode ser-lhe fornecido em outros suportes que garantem a total mobilidade e lhe proporcionam o facilidade de assinar documentos independentemente do computador onde está a trabalhar.

O suporte mais comum é o Cartão com Chip que pode armazenar o seu Certificado Digital. Para utilizar o seu Certificado que se encontra num cartão com chip terá que ter um leitor destes cartões.

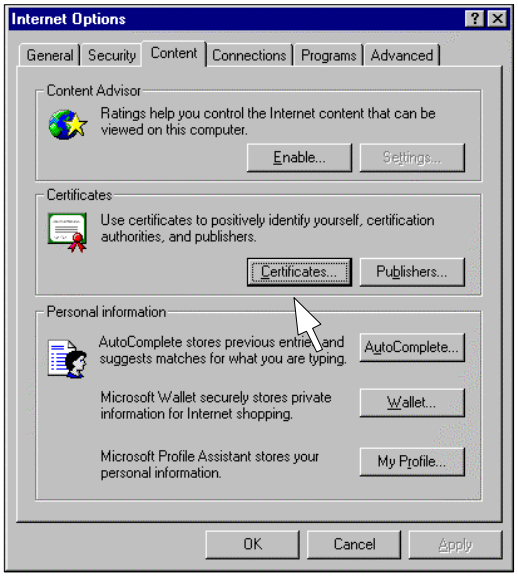
IA.1 - Uma vez aberto o browser, clique em *Tools (Ferramentas) -> Internet Options (Opções da Internet)*

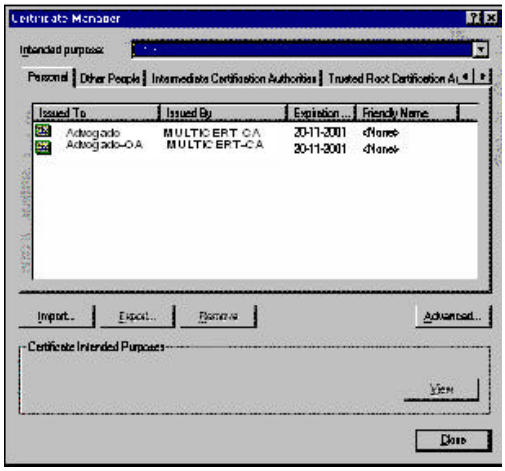


Irá surgir a janela:
Abra a pasta *Content (Conteúdo)*;



IA.3 Clique em *Certificates (Certificados)*

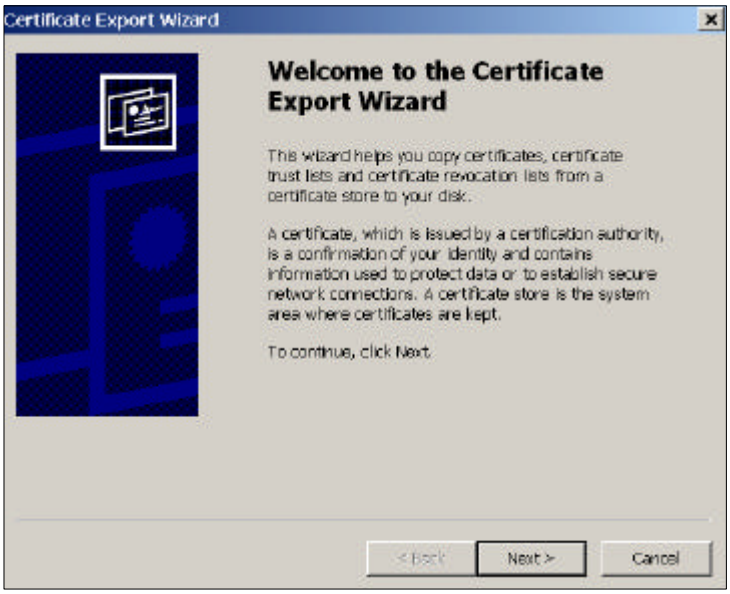




Seleccione o Certificado a exportar

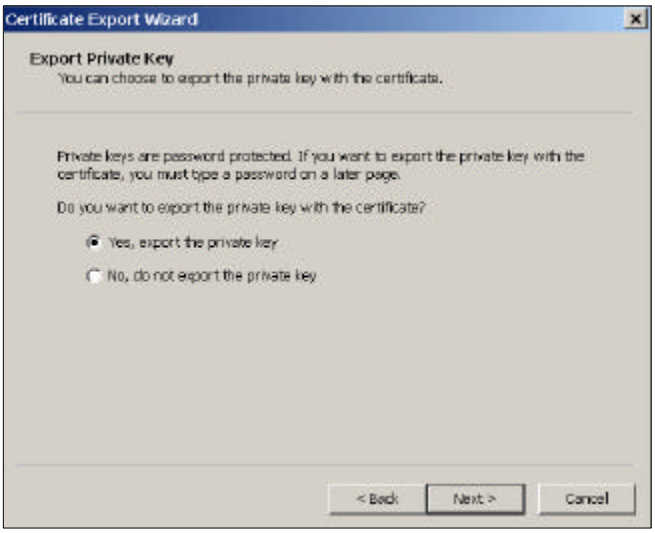
IA.4 - Vai agora exportar o Certificado, que se encontra já instalado no seu PC.

Clique *Export (Exportar).* Deverá seguir as instruções, conforme as seguintes figuras :

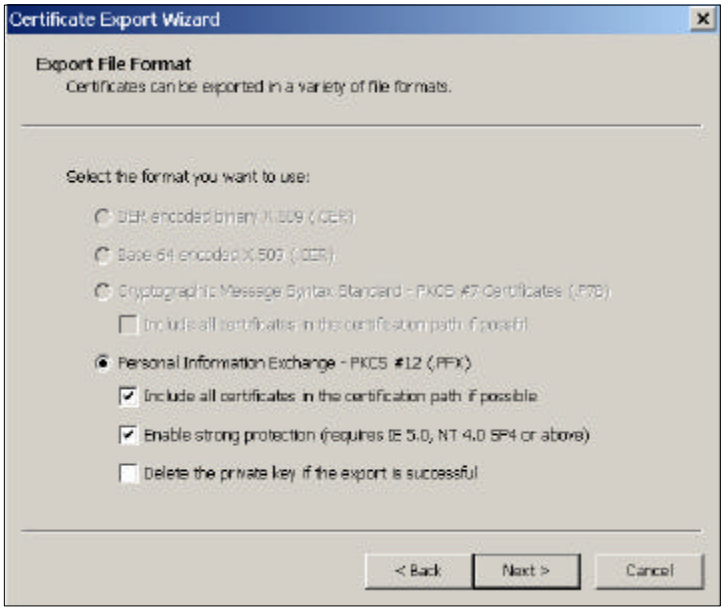


IA.5 Clique *Next (Próximo)*

IA.6 – Deve agora indicar que pretende exportar a chave privada, escolhendo a opção *Yes, export the private key (Exportar a chave privada)*.

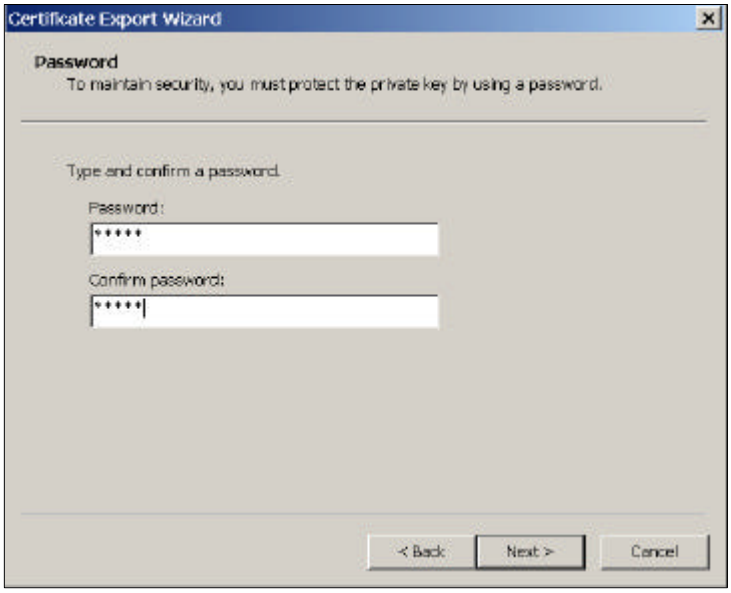


IA.7 – Agora tem que escolher a opção *Personal Information Exchange – PKCS #12 (.PFX)* , que é a única opção que deve escolher aqui.

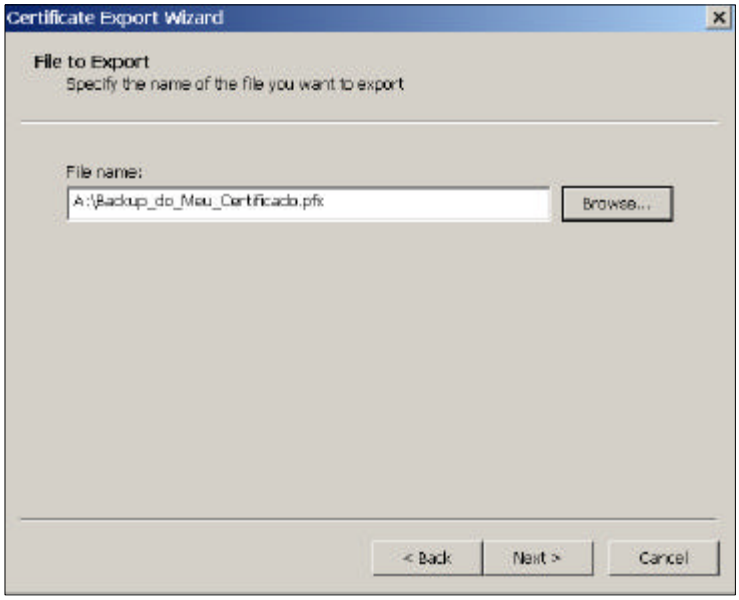


Tem que escolher as opções seleccionando as opções *Include all certificates in the path if possible (Incluir toda a cadeia de certificados, se possível)* e *Enable strong protection (Activar Protecção forte).* Deve ter em atenção que nunca deve seleccionar a opção *Delete the private key if expor tis sucessful (Apagar a chave privada, se a exportação tiver sucesso)*, visto que ao apagar a chave privada vai também remover o Certificado do seu sistema, tornando assim inválida qualquer operação que inclua assinatura ou identificação através do Certificado Digital.

IA.8 – Agora tem que definir a sua *Password (Palavra chave)* e confirmá-la. Tenha atenção que para conseguir importar este Certificado posteriormente, precisa de saber a password aqui definida (nada tem que ver com a password constante da carta de PIN. Pode escolher a passord que entender).



IA.9– Agora tem que escolher o nome do ficheiro e onde vai colocar esse ficheiro. Como este é uma cópia de segurança do seu Certificado, pode e deve guardá-lo numa disquete ou noutro suporte externo.



IA.10 Aqui aparece o ecrã a resumir as definições escolhidas durante o processo de exportação, pelo que deve carregar no Finish (Concluir), de forma a concluir a exportação.

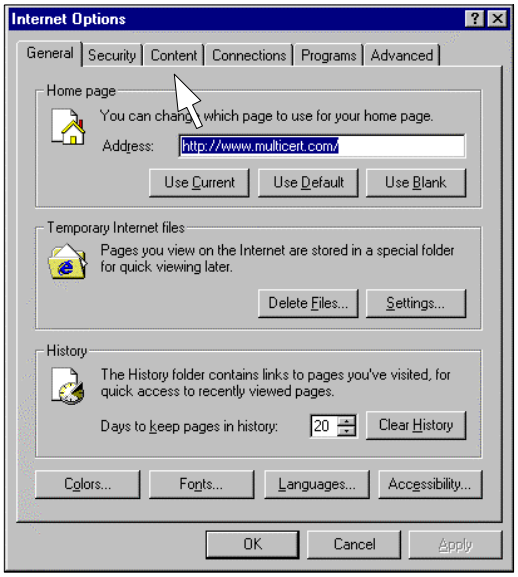
IA.11 Conclui com sucesso a exportação do Certificado. Agora deve guardar a disquete em local seguro, e protegida contra escrita.

Anexo IB – Importação dos Certificados

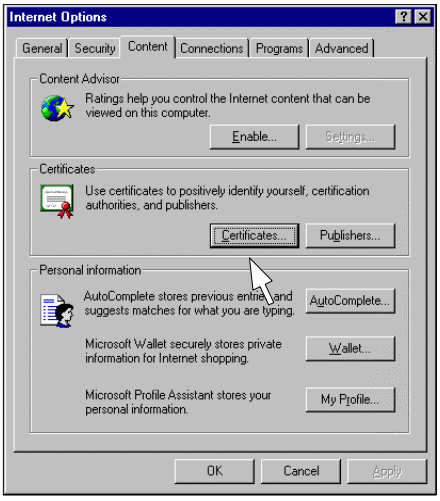
IB.1 - Uma vez aberto o browser, clique em *Tools (Ferramentas) -> Internet Options (Opções da Internet)*

Irá surgir a janela:

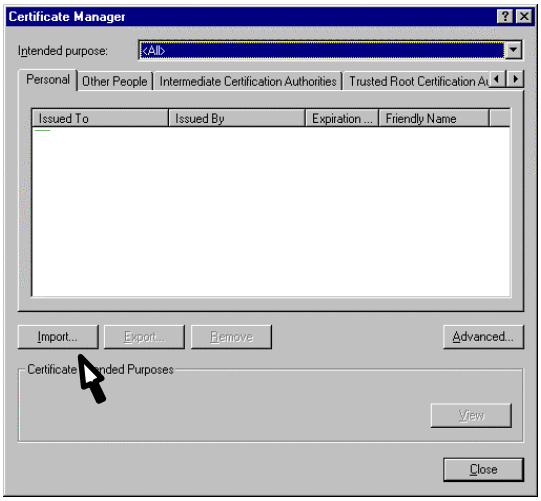
IB.2 Abra a pasta Content (Conteúdo);



IB.3 Clique em *Certificates (Certificados)*



Surge então a janela:

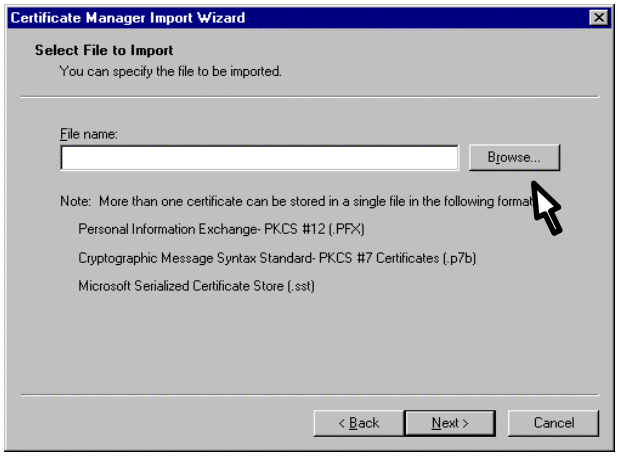


IB.4 - Vai agora importar o Certificado, que se encontra na disquete, para o seu PC. Clique *Import (Importar)*

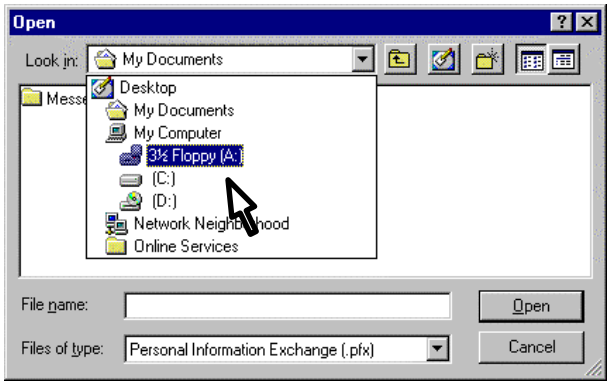
Deverá seguir as instruções, conforme as seguintes figuras:

IB.5 Clique *Next (Próximo)*

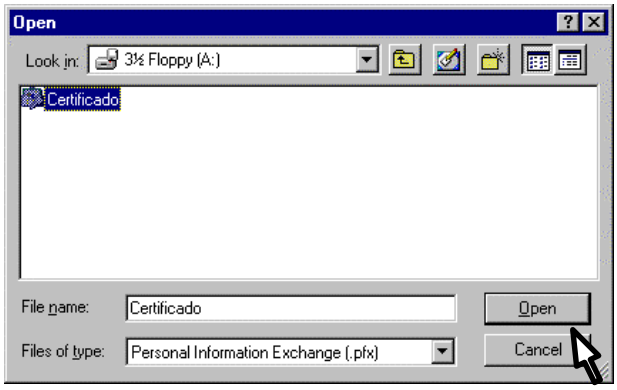
IB.6 - Vai agora indicar onde se encontra o seu Certificado. Introduza a disquete.



Clique *Browse (Procurar)*

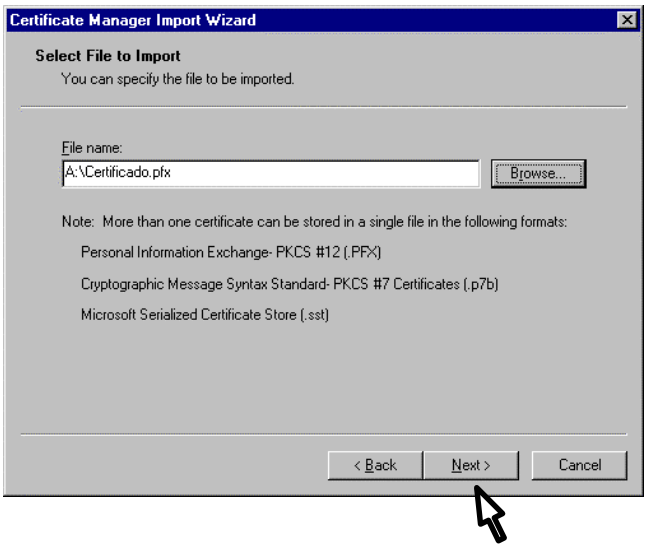


IB.7 - Uma vez seleccionada a disquete (drive A), seleccione o ficheiro que tem o Certificado.

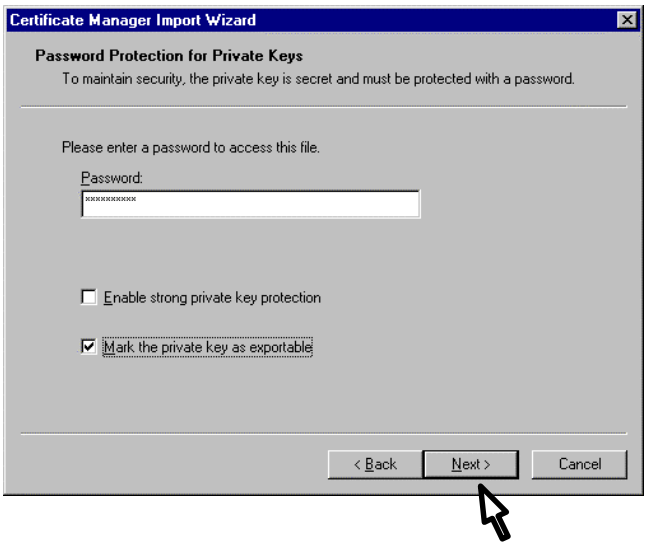


Este ficheiro tem o nome escolhido no momento da exportação feita anteriormente.

IB.8 - Clique *Open (Abrir)*, para confirmar.

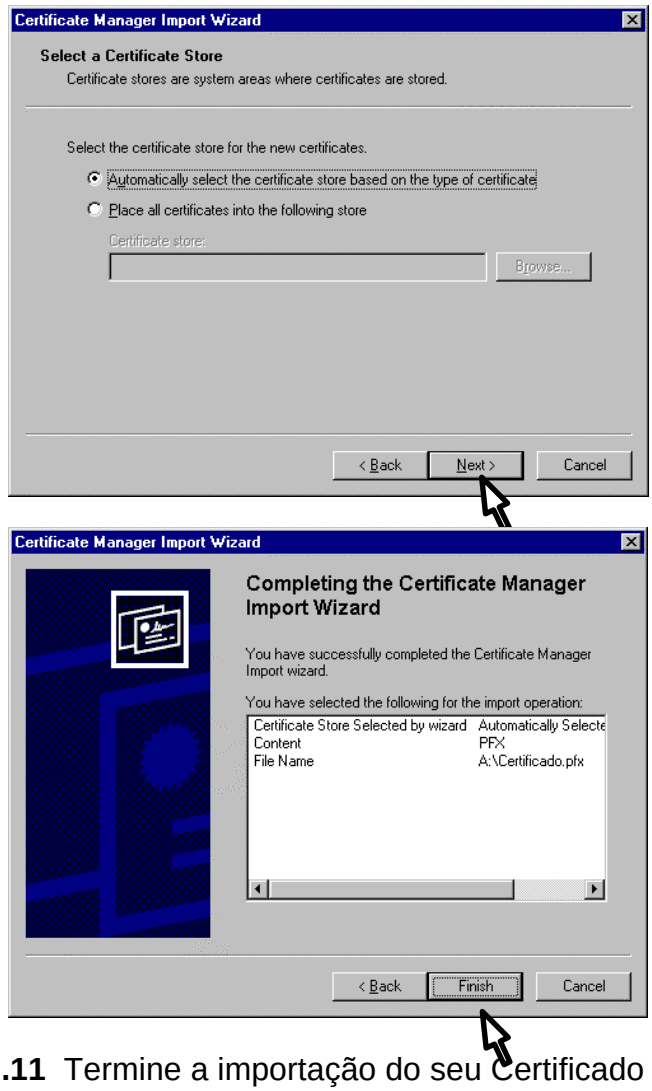


IB.9 - No campo *Password* deve escrever o código (PASSWORD) que escolheu anteriormente aquando da exportação do Certificado.



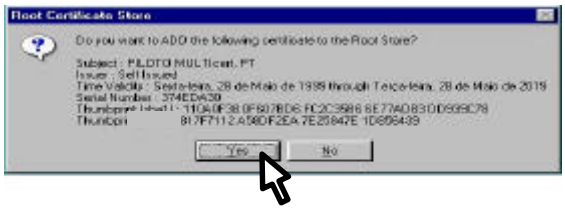
IB.10 Clique *Next (Próximo)*

Siga as instruções...



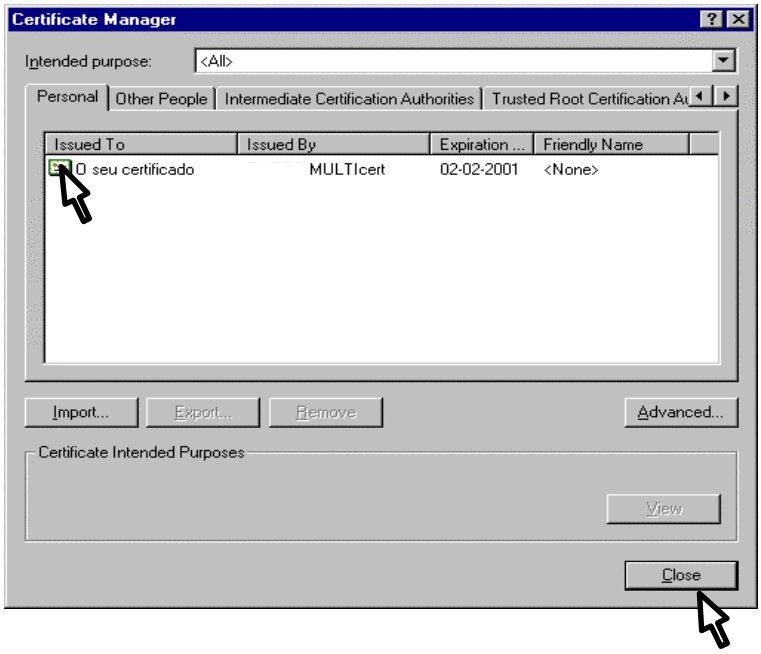
IB.11 Termine a importação do seu Certificado Digital.

Se os dados estão correctos então é só carregar no *Yes*, aceitando assim a importação.



Concluiu com sucesso a instalação do seu Certificado.

IB.12 Na janela seguinte pode verificar todos os certificados que se encontram instalados no seu browser.



Aqui consta o Certificado com o seu nome. Faça *Close (Fechar)*.

Se quiser consultar mais informação acerca do seu Certificado, basta fazer duplo clique sobre o mesmo.

Se quiser agora instalar o certifcado em outro computador, então passe ao capítulo **I – Configuração do Cliente de mail**

VI- Regime Jurídico aplicável

Legislação Aplicável:

Antes demais importa referir quais são os diplomas aplicáveis aos procedimentos adoptados neste manual:

- Decreto Lei n.º 290-D/99 de 2 de Agosto, que regula a validade, eficácia e valor probatório dos documentos electrónicos e a assinatura digital (artigo 1.º/1)

- Artigo 150.º do Código de Processo Civil, introduzido pelo Decreto-Lei 183/2000 de 10 de Agosto, que entra em vigor no dia 1 de Janeiro de 2003, podendo as partes dele prevalecer-se desde o dia 1 de Janeiro de 2001 (cfr. art.º 7.º do diploma mencionado)

- Portaria n.º 8-A/2001 de 3 de Janeiro, a produzir efeitos desde 1 de Janeiro de 2001

- Portaria n.º 1178-E/2000 de 15 de Dezembro, a vigorar desde 1 de Janeiro de 2001

Os procedimentos referidos neste manual centram-se essencialmente no artigo 150.º do Código de Processo Civil, cujo período de *vacatio legis* ainda não terminou. O referido artigo só entrará em vigor em 1 de Janeiro de 2003.

Nos termos do artigo 150.º/1 do Decreto-Lei acima referido, "1- Os articulados, alegações e contra-alegações de recurso devem ser apresentadas em suporte digital(...)".

A alínea c) do n.º 2 do mesmo artigo refere que as peças processuais podem ser enviadas para o tribunal através de correio electrónico.

No entanto, tal procedimento não é ainda suficiente, pois, se fosse assim tão simples poder-se-ia pôr em causa toda a validade do documento. Assim, a alínea c) do artigo 150º, n.º 2 exige que à mensagem enviada por correio electrónico seja aposta a assinatura digital do seu signatário.

Ou seja, será necessário que todos os Advogados adquiram um Certificado Digital, relacionando uma assinatura digital à sua identidade para que possam aceder a esta funcionalidade.

Mas, depois de todos estes procedimentos, ainda será necessário, de acordo com o n.º 3 do mesmo artigo 150.º, que as partes que utilizem este procedimento, enviem para a Secretaria do Tribunal no prazo de 5 dias a contar da data da expedição da mensagem por correio electrónico, a cópia de segurança, acompanhada dos restantes documentos que ainda não tenham sido enviados, bem como o comprovativo do prévio pagamento da taxa de justiça inicial, ou da concessão do benefício de apoio judiciário (150/4).

A cópia de segurança a que nos referimos no parágrafo anterior, nos termos do n.º 1 do artigo 150.º, será constituída por todos os documentos enviados em suporte digital, por correio electrónico, mas em papel. A cópia de segurança é uma exigência legal justificada pela necessidade de certificar que as cópias impressas no tribunal não sofreram alterações e correspondem na íntegra aos documentos enviados em suporte digital.

A Portaria n.º 1178-E/2000 de 14/11, vem por fim consagrar o dever de que os ficheiros enviados por correio electrónico sejam feitos em formato .RTF (rich text format), que é uma extensão de um formato utilizado pelo programa de tratamento de texto Microsoft Word.

A interpretação desta norma suscita desde logo a questão da imposição no formato dos ficheiros. A norma refere um dever e não uma obrigação. De todo

o modo, o formato .RTF tem a vantagem de permitir a abertura em qualquer processador de texto, ao contrário do que poderá acontecer com um documento gravado em formato .DOC.

No entanto, o formato .RTF poderá alterar toda a formatação dada ao documento.

Numa primeira análise, tal facto poderá parecer supérfluo, mas não é porquanto a forma dada a um articulado, o destaque dado a certas palavras, exercem um poder psicológico e de atenção a quem os lê e analisa. Em última instância, a forma, a apresentação e os destaques têm influência sobre quem decide.

Não queiramos pois comparar uma sentença manuscrita a uma dactilografada, ou uma dactilografada com letra de tamanho 8 e espaçamento de parágrafo simples, com uma com letra tamanho 12 e espaçamento 1,5... O mesmo efeito terão os articulados e requerimentos apresentados pelos ilustres causídicos.

Na Portaria n.º 1178-E/2000 de 14/11, bem como na Portaria n.º 8-A/2001 de 3 de Janeiro, exige-se a aposição de assinatura digital nos documentos enviados via correio electrónico (E-mail), nos termos do Decreto Lei n.º 290-D/99 de 2 de Agosto.

Esta exigência prende-se com a necessidade de atestar a inviolabilidade da informação enviada para o Tribunal. Ao apor uma assinatura digital num email o seu remetente está a garantir que a informação enviada vai chegar ao seu destinatário com a certificação de que não foi violado, pois caso o seja essa situação é alertada.

Traçado o regime jurídico, impõe-se a sua interpretação e aplicação prática.

Da letra da lei não se levantam grandes questões interpretativas. O mesmo não podemos dizer no que respeita à aplicação prática da interpretação dessas normas.

Aqui, todos nos detemos: Advogados e Tribunais. Todos esperam pelos outros. Os procedimentos estarão longe de ser únicos e unívocos. Soluções encontramos várias.

Se o envio de um simples fax para o Tribunal chega a originar duplicação e triplicação de documentos iguais nos processos, avolumando-os e enchendo-os de papeis desnecessários, imagine-se o que poderá acontecer com o envio desses mesmos requerimentos por email.

Levantam-se também questões não somenos importantes, como sejam a da certificação da recepção desses emails e dos documentos enviados em anexo. O pedido de envio de comprovativo de recepção pode ser, simplesmente, rejeitado pelo seu receptor.

Por outro lado, o envio desse recibo para o seu emissor originário carecerá igualmente de assinatura digital, para que deste modo aquele possa estar tranquilo quanto à origem e inviolabilidade desse recibo.

Por conseguinte, a simples impressão do email de envio não é suficiente para provar a prática do acto. De modo diferente acontecerá com o fax, estando este registado na Ordem dos Advogados e permitindo o aparelho a impressão de relatório de entrega.

Poderá parecer, então, que a solução legal, que procura ajustar a realidade da tecnologia e da inovação ao sistema judicial, tornando-o mais célere e eficaz, não seja mais do que uma medida burocratizadora e destituída de efeitos práticos, pois sempre se terá que enviar a cópia de segurança.

Contudo, não será bem assim. No termo de um prazo sempre será e é muito mais cómodo, prático e rápido (até mesmo económico) enviar um email com o requerimento ou articulado para o Tribunal competente e, em cinco dias, e com a tranquilidade que o cumprimento do acto nos traz, remeter ao tribunal a cópia de segurança em papel acompanhada de todos os documentos.

Outra questão de somenos importância prende-se com o cumprimento do artigo 229º-A do C.P.C., questionando-nos sobre a possibilidade das notificações entre mandatários poder ser ou não efectuada por correio electrónico.

Aqui devemos deter-nos com dois pontos essenciais para reflexão:

1. A ser possível a notificação entre mandatários por via de correio electrónico, deverão remetente e destinatário ser portadores de uma assinatura digital que ateste a inviolabilidade da informação remetida e recepcionada;
2. A prova do seu envio poderá estar dependente da remessa pelo destinatário de comprovativo de recepção assinado digitalmente.

Digamos que, de ora em diante (ou melhor, a partir de 1 de Janeiro de 2003) os Advogados poderão optar por remeter os seus requerimentos e articulados por email, beneficiando, se assim o entenderem, dessa comodidade e facilidade. Doutro modo, para aqueles que não virem vantagem ou comodidade neste processo, a lei impõe-lhes sempre a mudança: esse requerimento ou articulado terá sempre que ser entregue em suporte digital, ou seja, em CD-Rom, disquete ou correio electrónico.

O legislador inovou, forçou a mudança com a publicação do polémico Dec. Lei n.º 183/2000, que teve entrada em vigor no dia 1 de Janeiro de 2001. Para muitos a realidade, ou se preferirmos, a novidade por ele imposta era remota e até lá havia tempo para preparar todos os mecanismos necessários ao bom funcionamento dos desejados procedimentos.

A verdade é que, a pouco menos de 3 meses da derradeira data, ainda pouco se sabe sobre o que e como vai acontecer.

Em conclusão, da lei resultam estas máximas:

1- Os requerimentos ou articulados enviados para os tribunais têm ser entregues em suporte digital, devendo ser apresentados no formato RTF;

2- No caso daqueles serem remetidos por correio electrónico terão sempre que ter apostos uma assinatura digital;

3- A data de expedição conta como a data de prática do acto, mas aqui levantar-se-ão problemas com a prova da prática do acto caso não seja enviado comprovativo de recepção, devendo este igualmente ter aposta assinatura digital, embora esta seja uma interpretação que não resulta do dispositivo legal, mas que se impõe para uma maior credibilidade das relações entre os intervenientes, bem como questões de segurança e estabilidade do sistema judicial.

4- Envio no prazo de 5 dias da cópia de segurança e restantes documentos não digitalizados para a secretaria do tribunal.